UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/509,545	09/24/2004	Nobuyuki Watanabe	9683/205	5858

79510 7590 06/23/2008

NTT Mobile Communications Network I/BHGL
P.O. Box 10395
Chicago, IL 60610

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/509,545	WATANABE ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,15-19 and 21-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,15-19 and 21-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/04/2008, 02/26/2007, 08/16/2006, 09/022005, 12/21/2004, 09/24/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the original filing of September 24, 2008. Claims 5-14 have been cancelled by the preliminary amendment, thus claims 1-4, 15-19 and 20-23 are pending and have been considered below.

Preliminary Amendments

2. Acknowledge is made to preliminary amendment filed on September 24, 2004.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 01/04/2008, 02/26/2007, 08/16/2006, 09/02/2005, 12/21/2004 and 09/24/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

4. Claim 1 is objected to because of the following informalities: line 2 recites the limitation of " information providing server unit", the examiner suggests using " a first information providing unit"; line 6 recites the limitation of "another information providing unit', the examiner suggests "a second information providing unit". Appropriate correction is required.

5. Claim 1 is objected to because of the following informalities: claim 1 is a method claim, however applicant refers back to each step in the claim as a process. Appropriate correction is required.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-2, 4, 15-17 and 21-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Lin et al (US 6,766,53).

Claim 1: Lin et al discloses a transmission method comprising:

i. a process for a transmission system comprising

ii. an information providing server unit storing an entity file containing software for achieving an application(*Fig, item 208*);

iii. an administering server unit storing a security descriptive file containing authorization information showing authorization given to an application achieved when a terminal unit executes said software(*the security domain determines which of the client device's resources 212 the application will be allowed to access when running in the virtual machine environment) (column 3, lines5-10, column 3, lines 35-43:Fig.2, item, 210*); and

iv. another information-providing server storing an application descriptive file having contents dependent upon said entity file(*Fig. Item 206*), into which a storage location of said entity file and a storage location of said security descriptive file are written() (*column 3, lines 30-35: Fig. 3,*

item 302), the process for transmitting an application descriptive file to a terminal unit when a storage location of said application descriptive file is notified by said terminal unit(*the network address of the signed ADF is then made available so that client devices can download it to begin the installation and authentication procedure for the JAR file indirectly explaining transmitting ADF to the terminal*)(column 4, lines18-30);

v. a process for said terminal unit to notify to said transmission system a storage location of said security descriptive file contained in the application descriptive file transmitted from said transmission system(*the client device obtains the network location of the application code or JAR file, and transmits a request to the server, specifying the particular application desired (610)) column 5, 1-30)*;

vi. a process for said transmission system to transmit to said terminal unit said security descriptive file with security assured on the basis of the storage location of said notified security descriptive file(*a security policy file and a license policy file may be provided to describe what resources the application will need, what it will create, and the limitation on the use of the application as well as the transferability of the application.) (column 5, lines 30-51)*;

vii. a process for said terminal unit to notify to said transmission system said storage location of an entity file contained in said application descriptive file transmitted from said transmission system*(the client device*

obtains the network location of the application code or JAR file, and transmits a request to the server, specifying the particular application desired (610)) column 5, 1-30); and

viii. a process for said transmission system to transmit to said terminal unit said entity file on the basis of the storage location of said notified entity *file (The server transmits the application code to the client device (612)(column 5, lines 1-30).*

Claim 2: Lin et al discloses a terminal unit comprising:

ix. a communication unit for carrying out communication with a unit in

x. a network(Fig. 1, item 106);

xi. a storage unit (Fig. 2); and

xii. a controller,

wherein said controller comprises:

xiii. means for transmitting by said communication unit to a transmission system in said network a first transmission request to receive an application descriptive file from an information providing server in said transmission system and storing the application descriptive file in said storage unit(*to begin the method, the client device transmits (602) a request to a distribution server for the application)(column 4, lines 55-67)*, the first transmission request containing information on a storage location of the application descriptive file, the application descriptive file containing information on a storage location of an entity file containing software for

achieving an application(*the client device obtains the network location of the application code or JAR file, and transmits a request to the server, specifying the particular application desired (610))(column3, lines 20-35; column 5, 1-30)*, and information on a storage location of a security descriptive file containing authorization information showing authorization given to an application achieved by executing said software(*the ADF contains a pointer to the network location of the application in the file hash 304, an indication of the amount of memory space required to execute the application, and the environment necessary for execution)(column3, lines 25-35)*;

xiv. means for transmitting by said communication unit to said transmission system a second transmission request to receive a security descriptive file, the second transmission request containing information on a storage location of the security descriptive file, contained in an application descriptive file received from said transmission system (*The ADF contains a pointer to the network location of the application in the file hash 304, an indication of the amount of memory space required to execute the application) (column 3, lines 25-35);*

xv. means for transmitting by said communication unit to said transmission system a third transmission request to receive an entity file from an information providing server in said transmission system *(to begin the method, the client device transmits (602) a request to a distribution*

server for the application)(column 4, lines 55-67), the third transmission request containing information on a storage location of the entity file contained in an application descriptive file received from said transmission system(*ADF 302 describes the resources which are required by the client device, and may include a security policy file 314 or a license policy file 316, or both.)(column3, lines 25-35);* and

xvi. means for restricting, when execution of software contained in an entity file stored in said memory unit is commanded, operation of an application achieved by execution of said software, in accordance with authorization information contained in a security descriptive file corresponding to said entity file *(the security policy contains the information regarding which resources the application needs permission to use, as well as the names of files the application may create, and the network addresses it may need to access. The license policy may be used to set how the application may be used, such as whether it has a finite number of uses, or a finite period of time, whether it may be transferred to other users, and so on) (column 3, lines 30-45).*

Claim 4: Lin et al discloses a terminal unit as in claim 2 above, and further discloses wherein said controller receives said security descriptive file by said communication unit via a communication path whose security is assured(*column 3, lines 20-30).*

Claim 15: Lin et al discloses a terminal unit as in claim 2 above, and further

discloses wherein said application descriptive file contains a public key of a communication provider which provides communication service to said terminal unit (*developers provides their public key in the signed ADF so that client devices can use them to further establish a trusted chain) (column 5, lines 240-45),* wherein said security descriptive file is signed by a secret key of said communication provider *(the developer signs the concatenated file (406), by adding the developer's digital signature (element 312 from FIG. 3), and the ADF is fully signed)(column 3, lines64 to column 4, line 28*), and
wherein said controller inspects authenticity of a security descriptive file transmitted by said transmission system using a public key contained in said application descriptive file and notifies a storage location of said entity file to said transmission system only when said authenticity is proved (*if the hash of the application received in the signed ADF matches the hash of the received application file (in step 612), the client device loads the application into the virtual machine environment for execution according to the security and license policies, if any were present in the ADF) (column 4, line 54 to column 5, line 30*).

Claim 16: Lin et al discloses a terminal unit as in claim 2, and further discloses wherein said application descriptive file and said security descriptive file contain an application identifier assigned to a corresponding application*(file hash 304 of the JAR file) (column 3, lines 22-35)* and wherein said controller compares an application identifier contained in an application descriptive file transmitted by said transmission system to an application identifier contained in a security

descriptive file transmitted by said transmission system, and notifies a storage location of said entity file to said transmission system only when both identifiers match (*if the hash of the application received in the signed ADF matches the hash of the received application file (in step 612), the client device loads the application into the virtual machine environment for execution according to the security and license policies, if any were present in the ADF) (column 4, line 54 to column 5, line 30*).

Claim 17: Lin et al discloses a terminal unit as in Claim 2 above, and further discloses wherein said controller notifies a storage location of said security descriptive file to said transmission system only when a storage location of said security descriptive file written in said application descriptive file is inside said administering server unit system (*The ADF contains a pointer to the network location of the application in the file hash 304, an indication of the amount of memory space required to execute the application) (column 3, lines 25-35).*

Claim 21: Lin et al discloses a transmission system comprising:

xvii. one or a plurality of server units wherein an entity file, a security descriptive file and an application descriptive file are stored(Fig. 2), the entity file containing software for achieving an application, the security descriptive file containing authorization information showing authorization given to an application achieved by executing said software, and application descriptive file having contents depending upon said entity file into which storage locations of said entity file and said security descriptive

file are written *The ADF contains a pointer to the network location of the application in the file hash 304, an indication of the amount of memory space required to execute the application) (column 3, lines 25-35).*, wherein a server unit among said one or a plurality of server units in which said security descriptive file is stored is an administering server unit to which authorization for administering a security descriptive file is given(*ADF 302 describes the resources which are required by the client device, and may include a security policy file 314 or a license policy file 316, or both.)(column3, lines 25-35)*, wherein each of said server units comprises a means for returning to an originator of notification a file when a storage location of said file is notified *file (The server transmits the application code to the client device (612)(column 5, lines 1-30)*, and wherein said administering server unit, when a storage location of said security descriptive file is notified, returns said security descriptive file to an originator of notification with security assured (*column 3, lines 20-30).*.

Claim 22: Lin et al discloses an administering server unit comprising:

xviii. a communication unit(Fig. 1);

a storage unit (Fig. 2); and

a controller which carries out,

xix. a process for writing into said storage unit a security descriptive file containing authorization information showing authorization given to an application, the application is achieved by executing software(*to begin the*

method, the client device transmits (602) a request to a distribution server for the application)(column 4, lines 55-67),

xx. a process for writing information on validity of said security descriptive file into said storage unit*(column 4, line 54 to column 5, line 30)*, and

xxi. a process, when inquiry about validity of said security descriptive file is received by said communication unit from a terminal unit, for reading out information on validity of said security descriptive file from said storage unit, and notifying to said terminal unit the information by said communication unit match (*if the hash of the application received in the signed ADF matches the hash of the received application file (in step 612), the client device loads the application into the virtual machine environment for execution according to the security and license policies, if any were present in the ADF) (column 4, line 54 to column 5, line 30*).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al (US 6,766,353) in view of Carpenter et al (US 6,976,165).

Claim 3: Lin et al discloses a terminal unit as in claim 2 above, and further A terminal unit of Claim 2, but does not explicitly discloses wherein said transmission system assures security by transmitting to said terminal unit said security descriptive file after encrypting, nor wherein said controller comprises a means for decrypting an encrypted security descriptive file transmitted by said transmission system. However, Carpentier et al discloses a terminal for secure storage transfer and retrieval of content, which further discloses:

xxii. wherein said transmission system assures security by transmitting to said terminal unit said security descriptive file after encrypting(Fig. 3; FIG.4), and

xxiii. wherein said controller comprises a means for decrypting an encrypted security descriptive file transmitted by said transmission system(Fig. 4, Fig. 9A, item 626).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Lin et al such as to encrypt and decrypt security file One would have been motivated to do so in order to securely store transfer and retrieve information using related techniques as taught by Carpentier et al (column 1, line10-17).

9. Claims 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al (US 6,766,353) in view of Wolf (US 5,673,315).

Claim 18: Lin et al discloses a terminal unit as in claim 2 above, and further discloses wherein said security descriptive file contains time limit information showing an expiration date of a corresponding application(*validity period)(column 3, lime 53-65; Fig. 3, item 310*), and said controller comprises a means for repeatedly receiving said security descriptive file in a chronological order from said transmission system by repeatedly notifying a storage location of said security descriptive file to said transmission system in a chronological order(*the ADF contains a pointer to the network location of the application in the file hash 304, an indication of the amount of memory space required to execute the application, and the environment necessary for execution)(column3, lines 25-35)*; but does not explicitly discloses a step of renewing an expiration date of said application on the basis of said time limit information contained in said security descriptive file repeatedly received. However, Wolf discloses a terminal for software asset usage detection, which further discloses a step of renewing an expiration date of said application on the basis of said time limit information contained in said security descriptive file repeatedly received(column 2, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Lin et al such as permit the renewal of application One would have been motivated to do so in order to prevent software piracy and unauthorized uses.

Claim 19: Lin et al and Wolf disclose a terminal unit as in claim 18 above, and Wolf further discloses wherein said terminal unit renews an expiration date of

said application only when said security descriptive file is properly transmitted from said transmission system. (column 2, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Lin et al such as permit the renewal of application One would have been motivated to do so in order to prevent software piracy and unauthorized uses.

10. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al (US 6,766,353) in view of Barnett (US 6,971,016).

Claim 23: Lin et al discloses a terminal unit comprising:

i. a communication unit(Fig. 1);

ii. a storage unit(Fig. 2); and

iii. a controller which carries out,

iv. a process for receiving from an administering server unit a security descriptive file containing authorization information showing authorization given to an application, the application is achieved by executing software, and writing said security descriptive file into said storage unit (*the server transmits the application code to the client device (612)) (column 4, line 64 to column 5, line 6),*

v. a process for repeatedly transmitting to said administering server unit by said communication unit inquiry about validity of a security

descriptive file stored in said storage unit*(column 4, line 54 to column 5, line 30*), and

but does not explicitly discloses a process, when a response that said security descriptive file has been voided is received from said administering server unit by said communication unit, for disabling activation of an entity file corresponding to said security descriptive file. However, Barnett discloses an authenticated access to storage area network, which further discloses a process, when a response that said security descriptive file has been voided is received from said administering server unit by said communication unit, for disabling activation of an entity file corresponding to said security descriptive file(column Fig. 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Lin et al such as to disable activation when software has been void . One would have been motivated to do so in order to implement a secure and cost effective mechanism for assuring the integrity of transaction as taught by Barnett (*column 1, lines 5-10*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Tuesday, June 17, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136